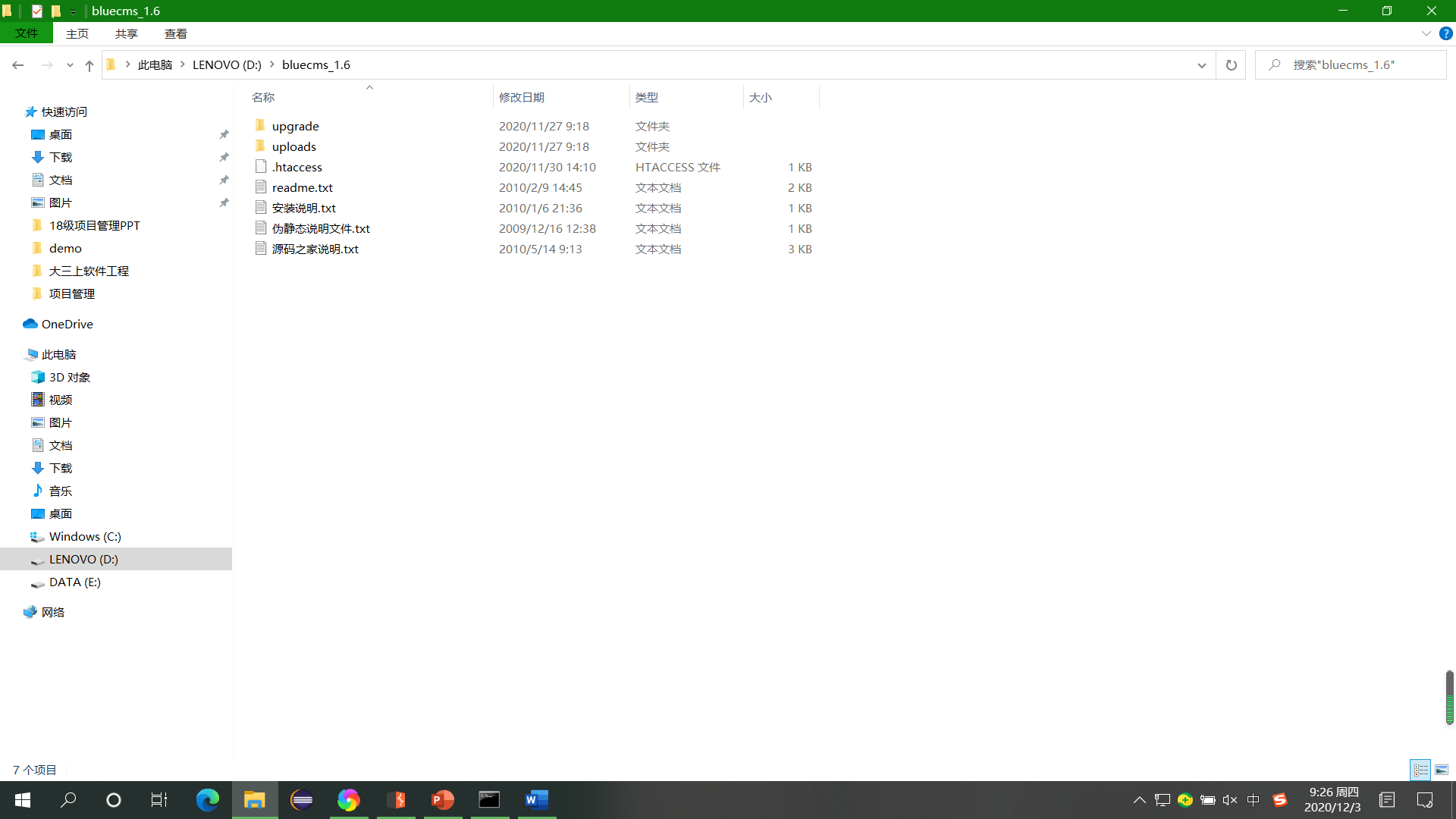
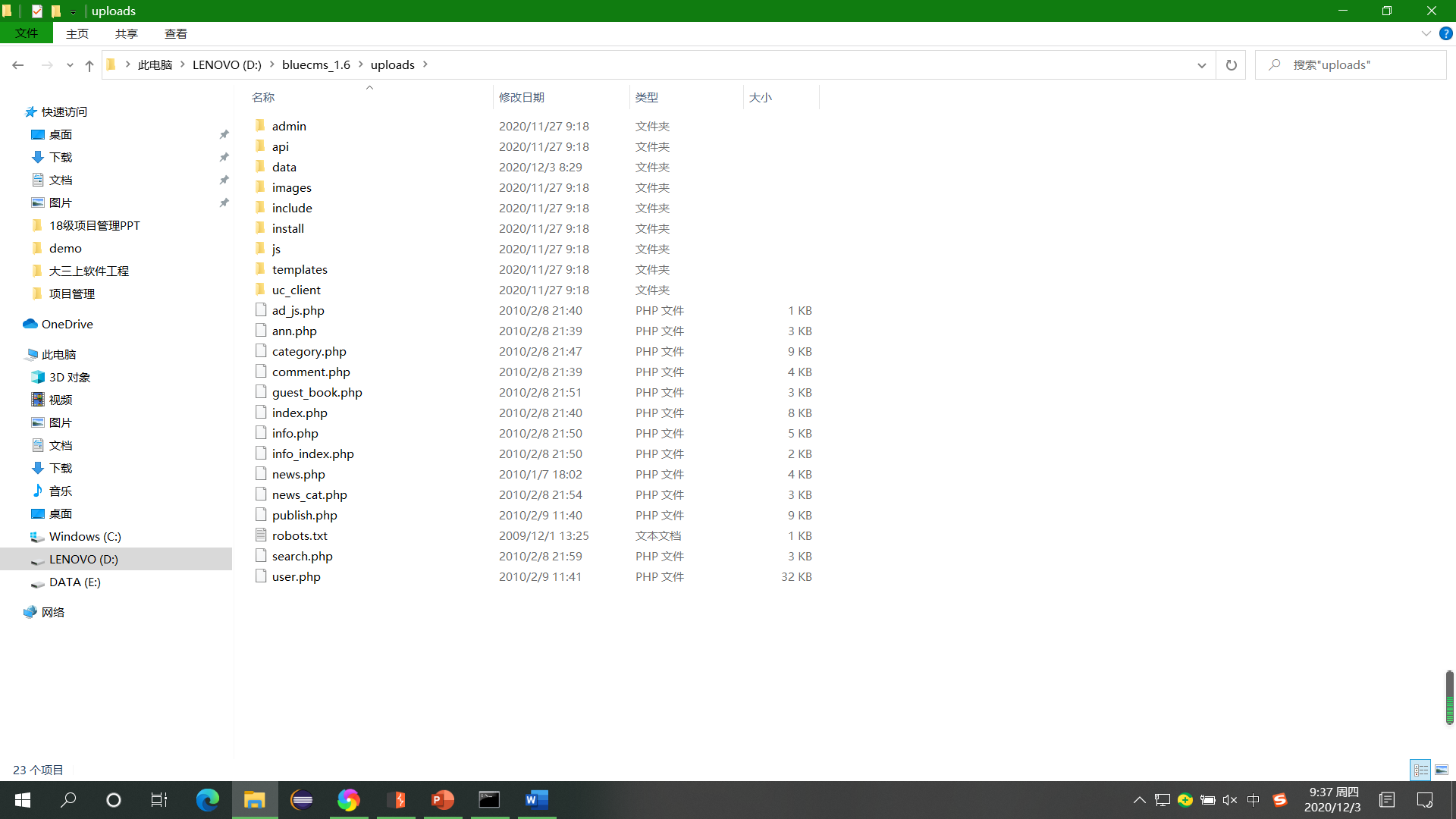
**渗透测试**

1. 信息收集
2. 域名信息

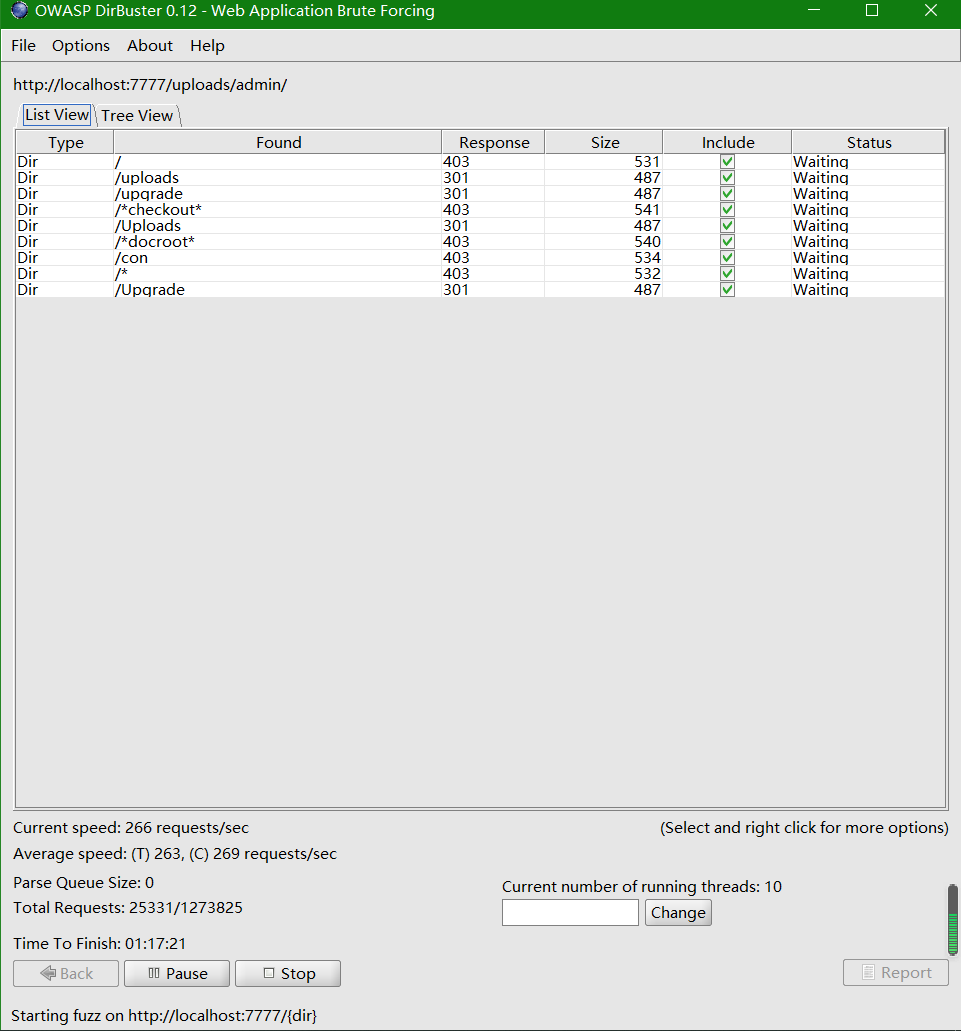
IP地址 10.7.86.241

1. 敏感目录

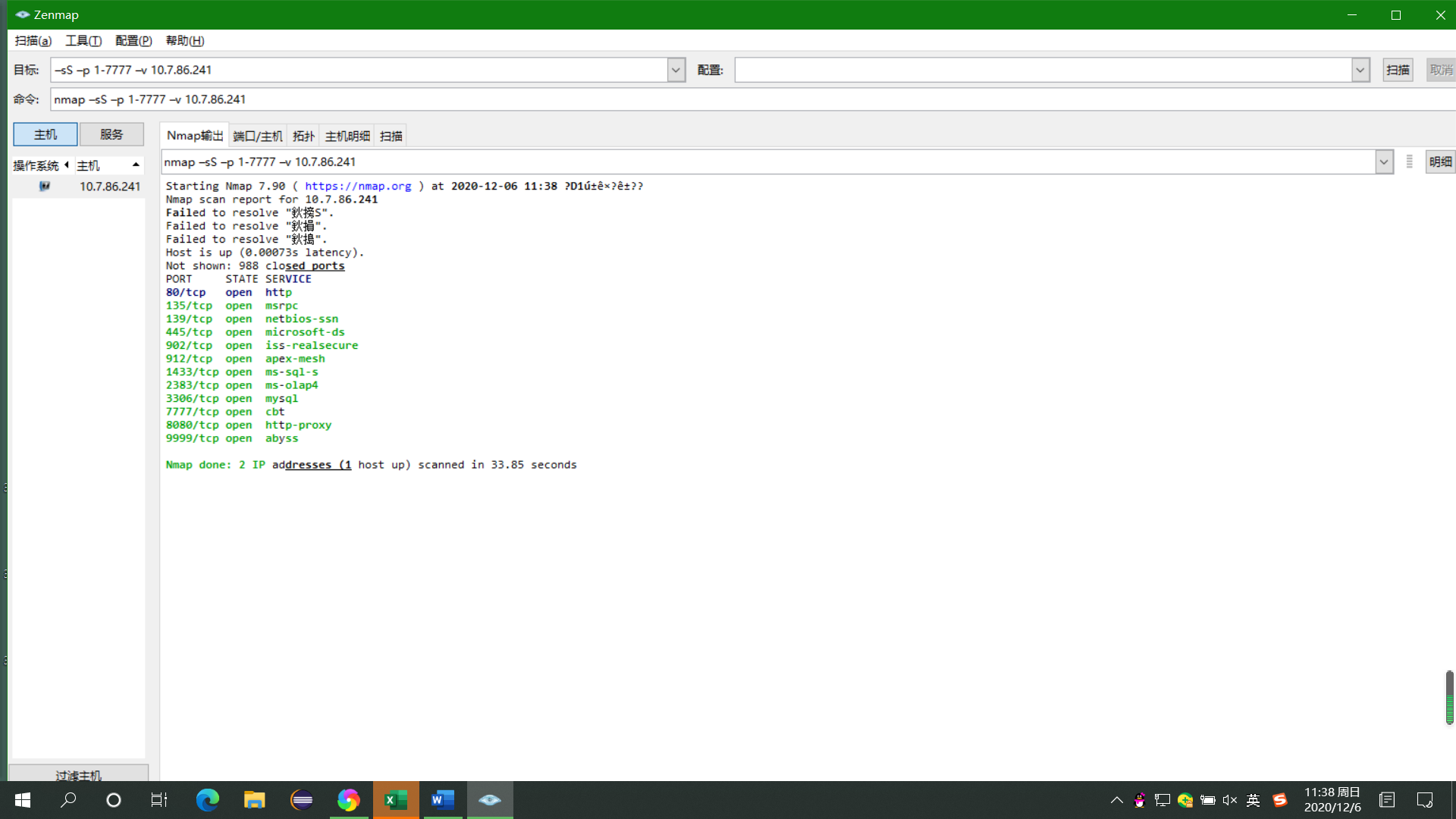


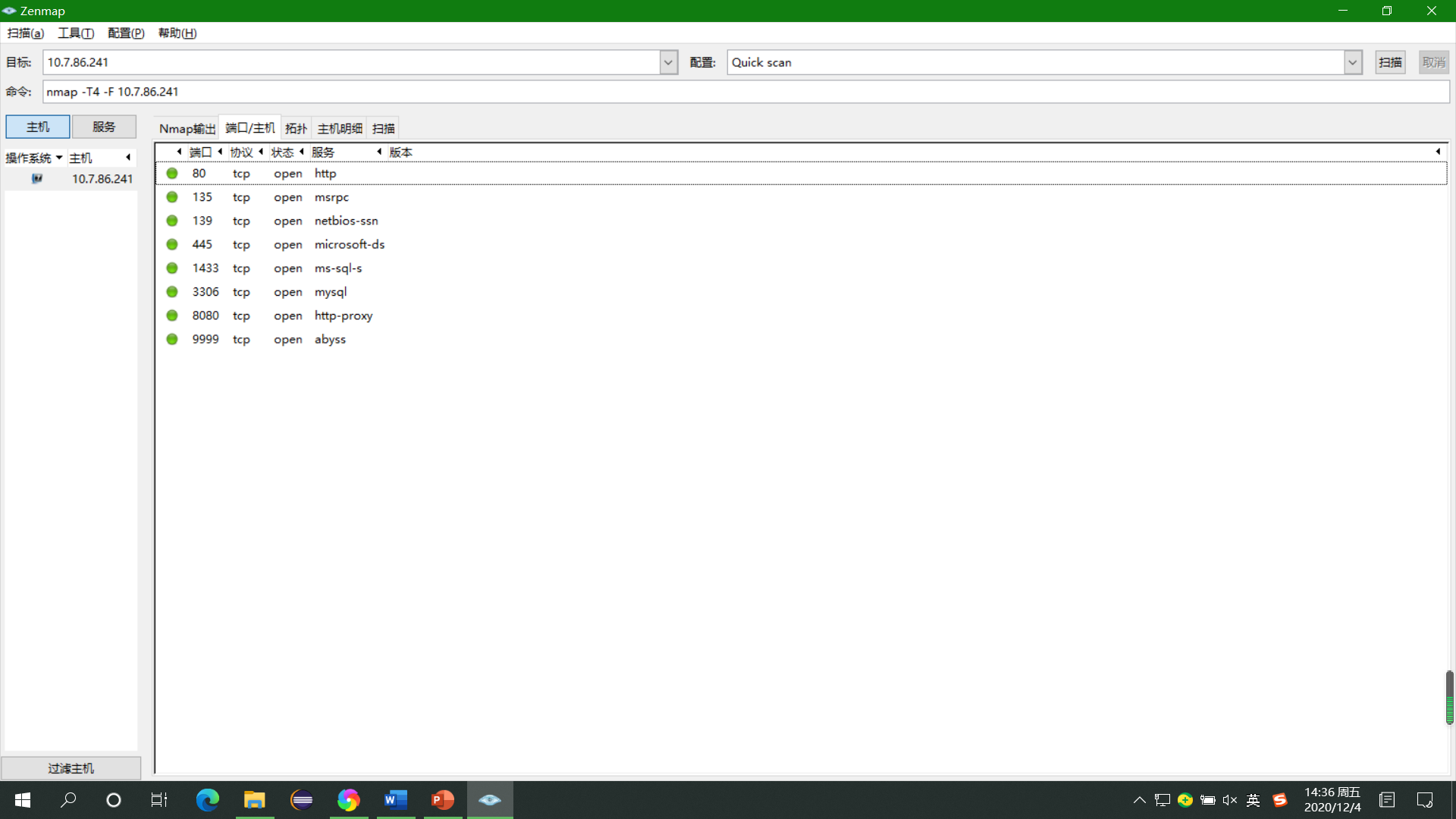


借助DirBuster工具进行敏感目录和隐藏文件的扫描：



借助Zenmap进行端口扫描：





1. 整站分析

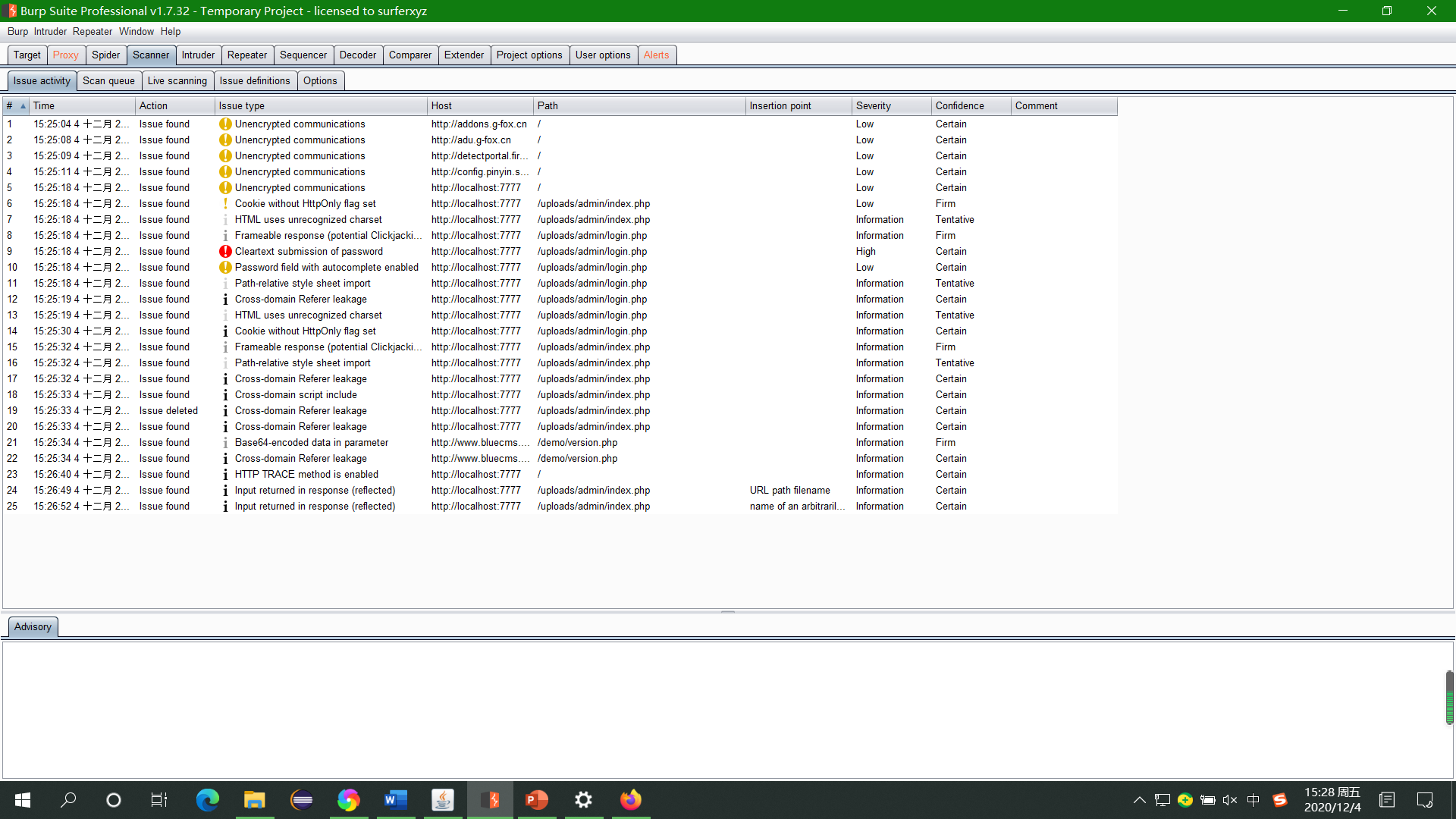
使用Windows系统，因为URL中字母大写仍能访问

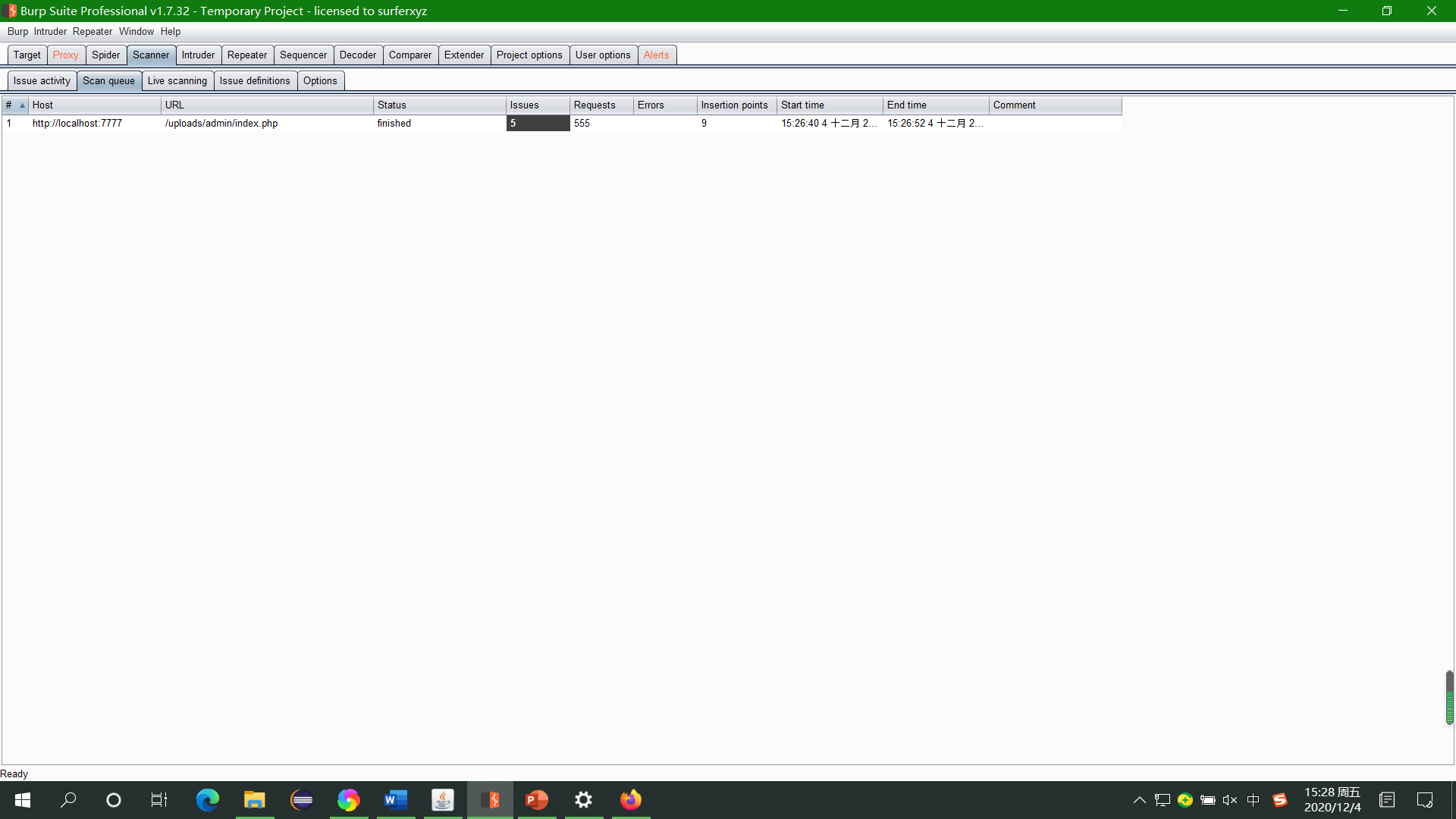
脚本类型PHP脚本，因为URL后有.php

服务器软件：Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod\_fcgid/2.3.9a

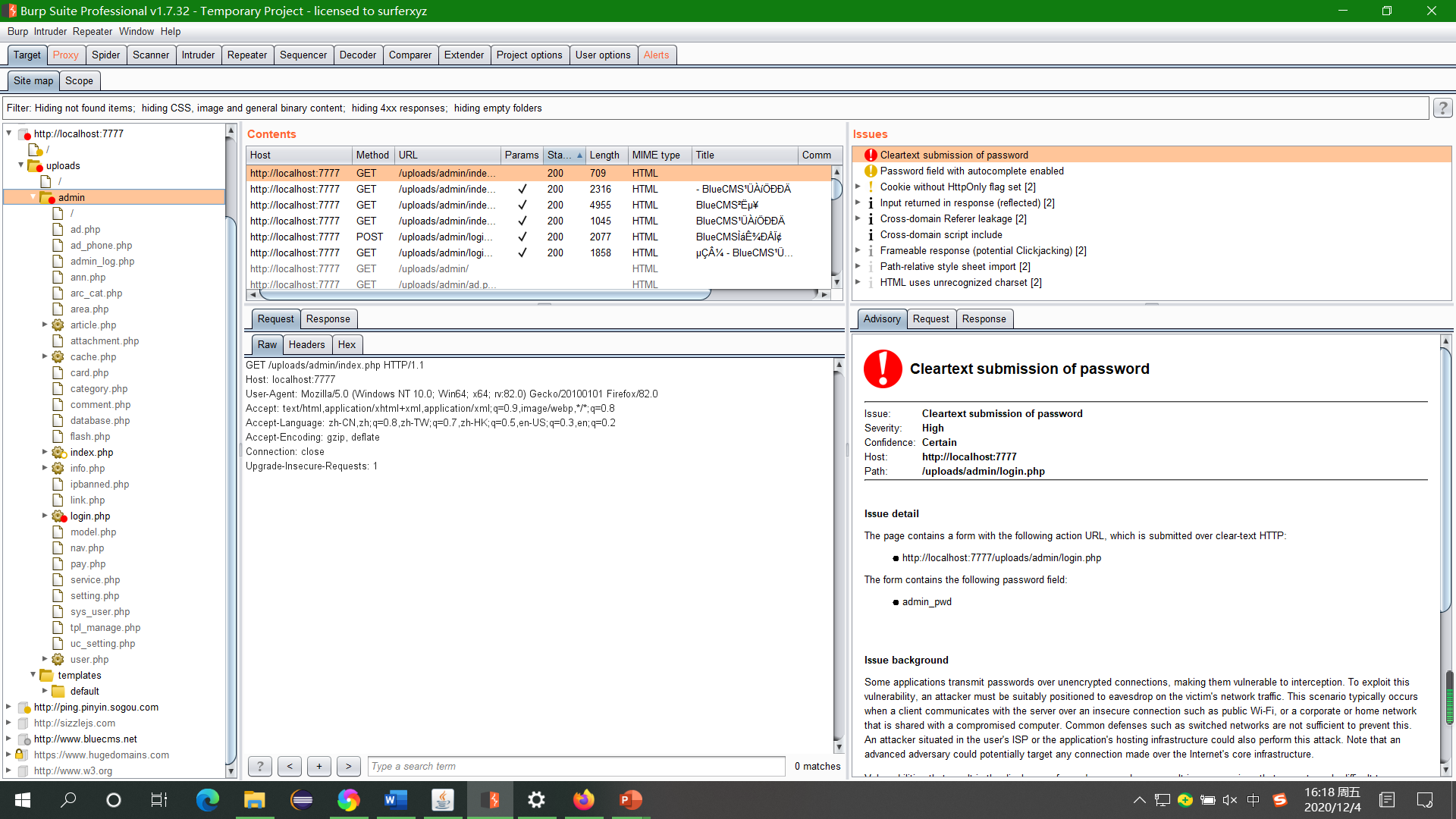
使用MySQL 版本5.7.26

1. 使用BurpSuite漏洞扫描



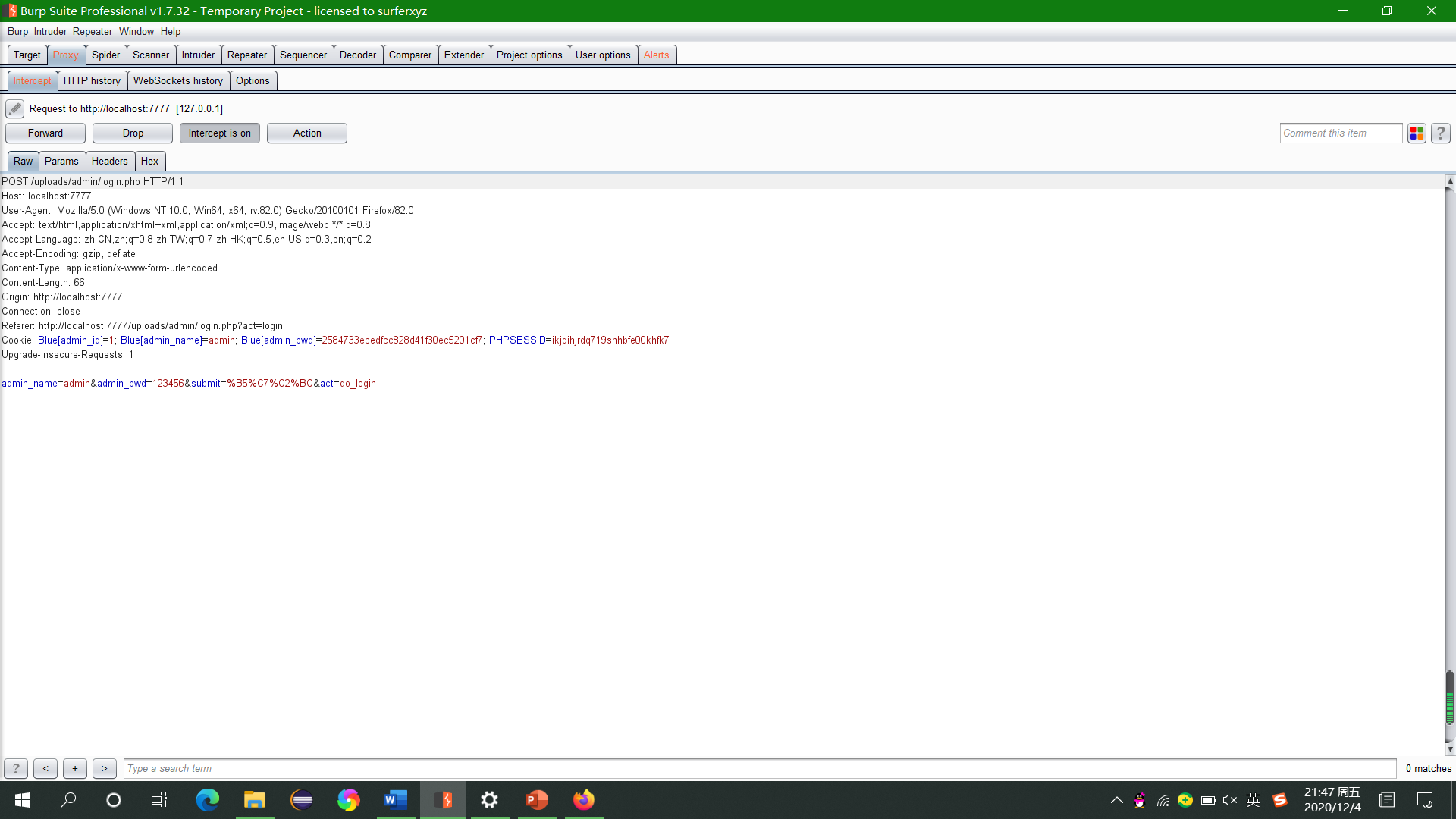


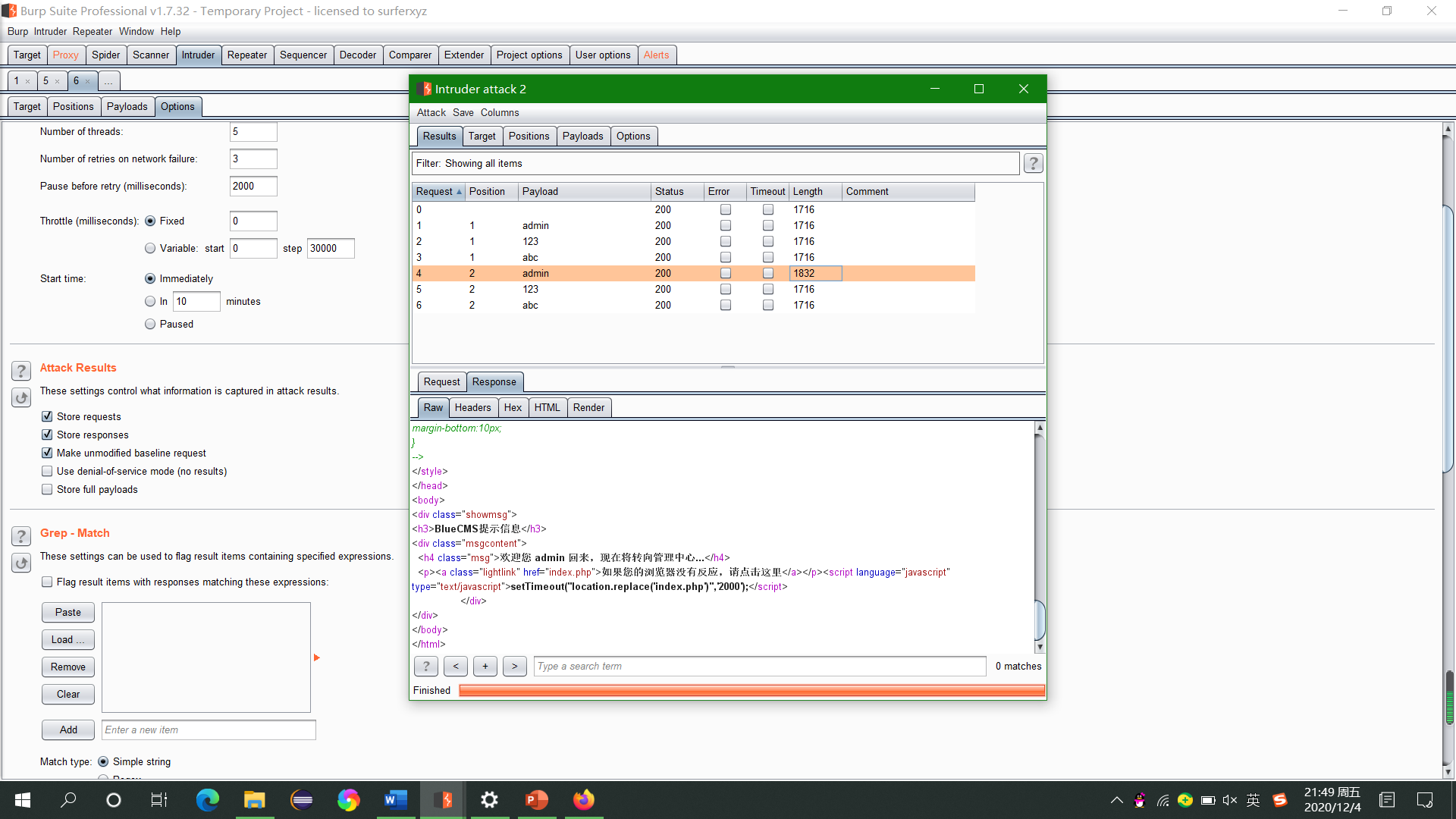
1. 爬取网站



抓包：

（1）Sniper





(2)Battering ram:

